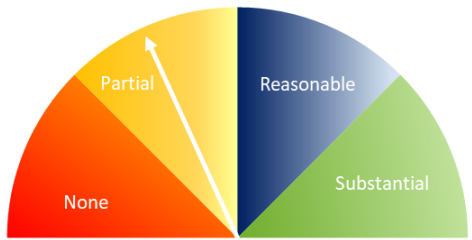


Compliance with the General Data Protection Regulation 2019/20

Draft Report

Issue Date: 14th February 2020

Executive Summary

Audit Opinion		Recommendation Summary	
	<p>In relation to the areas reviewed and the controls found to be in place, some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.</p>	Priority	Number
		Priority 1	0
		Priority 2	11
		Priority 3	4
		Total	15

Audit Conclusion
<p>The majority of the findings in this report stem directly from the absence of key roles during the implementation stages of GDPR, along with limited levels of ongoing involvement from key contacts at the administering authority, SCC.</p> <p>The allocation of responsibility to ensure GDPR compliance was achieved was incomplete. The former SWP Business and Governance Manager, who was responsible for GDPR readiness, left his post in August 2018.</p> <p>Whilst SWP were provided with some initial awareness training and support from the SCC Information and Governance Manager, he also left his post in January 2018 and there was no continuity of GDPR support from SCC. As a result, not all of the GDPR preparation required has taken place and our report includes a number of areas of non-compliance and has resulted in a partial opinion being given.</p> <p>These key roles have now been re-established with the SWP Business Support Manager now having GDPR responsibility and SCC resourced to be able to provide oversight and support. It is now important for SWP and SCC to draw up an action plan to address these areas of weakness. At the request of the SWP Managing Director, the Findings and Actions section of this report has been divided into recommendations to be implemented by the SCC Data Protection Officer and those to be implemented by the Waste Partnership.</p>

Background

The EU General Data Protection Regulation (GDPR) took effect on 25 May 2018. Together with the Data Protection Act 2018, which adopts the GDPR standards for all general data in the UK, it replaced the Data Protection Act 1998 (DPA 1998) and applies to the processing of **all** personal data. The legislation controls how personal data is used and processed by organisations.

In order to be compliant, Somerset Waste Partnership is required to adhere to the data protection principles outlined within the regulations. The principles set out the prerequisite for all organisations to ensure that personal information is:

- Used fairly, lawfully and transparently;
- Used for specific, explicit purposes;
- Used in a way that is adequate, relevant and limited to only what is necessary;
- Accurate and, where necessary, kept up to date;
- Kept for accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary.

Further to this, the Data Protection Act 2018 also outlines the rights of individuals to know what data is collected or held by organisations about themselves and how that data is processed.

Since the implementation of GDPR in May 2018, the Information Commissioners Office (ICO) are now able to apply fines for any contraventions under a two-tiered sanction scheme – with lesser incidents subject to a maximum fine of either €10 million (£7.9 million) or 2 per cent of an organisation’s global turnover (whichever is greater). The most serious violations could result in fines of up to €20 million or 4 per cent of turnover (whichever is greater).

A review has been undertaken to assess the extent to which the Waste Partnership adhere to the key principles of the GDPR, across their main areas of operation. This is especially crucial at a time when the Partnership is planning for the commencement of a contract with its new collections service provider, implementing a new customer relation management system, My Waste Services and also transitioning from a shared network drive to SharePoint in January 2020.

Corporate Risk Assessment

Objective

To verify the extent to which the organisation has implemented revised arrangements and resourced itself to comply with the legislation. This will include the transition arrangements with the new rights of individuals, handling subject access requests, consent, data breaches, and designating a data protection officer, under the General Data Protection Regulation.

Risk	Inherent Risk Assessment	Manager’s Initial Assessment	Auditor’s Assessment
------	--------------------------	------------------------------	----------------------

The updated control framework necessary for GDPR compliance has not been adequately planned, resourced and implemented, resulting in reputational and financial loss to the authority and negative consequences for data subjects.

High

Medium

Medium

Scope

Meetings were held with the following individuals:

SWP Business Support Manager

SCC Service Manager - Customer Experience and Information Governance (the Data Protection Officer)

SCC Enterprise Architect (Applications) – ICT Service.

We have reviewed the information published on the SWP website and a variety of other relevant documents, including the inter-authority agreement, contractual agreements with the main contractors and data protection impact assessments where available.

Findings and Outcomes

1. The updated control framework necessary for GDPR compliance has not been adequately planned, resourced and implemented, resulting in reputational and financial loss to the authority and negative consequences for data subjects.

Findings and Actions for the Data Protection Officer

1.1 Finding and Action

Issue	Risk
<p>The allocation of key responsibilities to ensure GDPR compliance has not been completed in a timely manner.</p>	<p>SWP will continue to be non GDPR compliant and moving forwards GDPR will not be considered as part of future business improvement projects.</p>
<p>Findings</p>	
<p>Public Authorities are required to designate responsibility for data protection compliance to an individual who has the knowledge, support and authority to do so effectively.</p> <p>Through discussion as part of this audit, it was established that the SCC Data Protection Officer (DPO) had not been formally assigned the role for DPO of SWP, since assuming the role from the previous postholder. It is now understood that the DPO role has been assumed, but the period during which the role was unfilled has resulted in some projects, such as the implementation of SharePoint and the My Waste Services system, not having DPO input.</p> <p>Furthermore, over this period SWP have not been kept updated on the actions completed by SCC to achieve corporate GDPR compliance, or provided with guidance on what they themselves needed to consider and therefore may have not received important information.</p>	
<p>Recommendation</p>	
<p>We recommend that the SCC Data Protection Officer engages with SWP to formulate an action plan to enable SWP to achieve GDPR compliance. This should include the following areas as per the additional recommendations made below:</p> <ol style="list-style-type: none"> 1. Record of Processing Activity and Privacy Notices (see 1.2, 1.3, 1.4) 2. Policy Framework (see 1.5) 3. Data Subject Access Requests (see 1.6) 4. 	<p>Priority Score</p> <p style="text-align: center; font-size: 24pt; font-weight: bold;">2</p>

Agreed Action	Timescale	Action plan in place by end of November 2020
<p>SCC are SWP’s administering authority and this includes data protection responsibilities. SWP requested this audit because we take this area seriously, and were conscious that we needed to ensure that we progressed the necessary actions to be fully GDPR compliant, and we wanted SWAP’s expertise to support us in developing an action plan. SWP understands that a Record of Processing Activity has not yet been fully completed for SCC as a whole.</p> <p>SWP engaged SCC’s Enterprise Architect during the work to implement My Waste Services, indeed SWP procured more time from the Enterprise Architect to ensure he was more fully involved in this process as we recognised that we needed a greater degree of expert input into this area than would normally be available from the administering authority through ‘business as usual’. SWP also engaged with SCC’s Data Protection Officer during this process and took legal advice on relevant aspects of this.</p> <p>SWP have met SCC’s Data Protection Officer to ensure that sufficient resources are allocated to support SWP with developing an action plan. It is anticipated that an action plan will be in place by the end of November 2020. In addition to the scope outlined above it will include ensuring that we have standardised processes for dealing with FOIs and complaints with all partners – as some partners do these in different ways at the moment.</p>	Responsible Officer	<p>SCC Data Protection Officer/ SWP Managing Director (Project managed by SWP Business Support Manager)</p>

1.2 Finding and Action	
Issue	Risk
No information audit has been conducted and there has been only limited consideration of all personal data collected, held and transmitted by the Waste Partnership.	Non-compliance with the GDPR may in the first instance result in a warning from the Information Commissioner's Office and could also result in reputational damage.
<p>Findings</p> <p>A Record of Processing Activity (ROPA) assessment is considered to be a best practice approach to consider and document all information transactions. Organisations also need to consider whether there is a possibility that they may hold any inaccurate personal data and have shared it with another organisation, meaning they will have to tell the other organisation about the inaccuracy so they can correct their own records. They will not be able to do this until they have assessed and documented all the sets of personal data they hold, where it came from and who they share it with. SWP have not completed a ROPA and this is an exercise that would be best completed with support from the SCC Data Protection Officer.</p> <p>It was also discussed with the SWP Business Support Manager what processes are in place to ensure that if a citizen contacts either their District Council or the Waste Partnership to advise they hold an inaccurate record of their name and/or address, how the corrected information is transmitted to the other party to ensure all records are updated. There is currently an incomplete understanding of how this process works and therefore, it should be reviewed for compliance. Doing this will also help to ensure compliance with the GDPR's accountability principle, which requires the authority to be able to show how they comply with the GDPR principles.</p> <p>The ROPA will help to ensure GDPR compliance by demonstrating that SWP have considered and recorded the following information:</p> <ul style="list-style-type: none"> * name and details of the organisation (and where applicable, of other controllers, the representative and data protection officer); * purposes of the processing; * description of the categories of individuals and categories of personal data; * categories of recipients of personal data; * details of transfers to third countries including documentation of the transfer mechanism safeguards in place; * retention schedules; and * description of technical and organisational security measures. <p>Completing the ROPA will also assist SWP in identifying the lawful basis for all data processing activities and document them. The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever they process personal data. The relevant bases for the collection of waste are likely to be:</p> <p><i>(d) Vital interests: the processing is necessary to protect someone's life; and</i></p>	

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

There are however instances where the Waste Partnership may need to be able to explain their lawful basis for processing personal data in their Privacy Notice(s), which will need to be completed in tandem with a review of Privacy Notices as recommended in 1.3.

Recommendation

We recommend that the SCC Data Protection Officer should work with the Waste Partnership to ensure that as part of completing the Record of Processing Activity, consideration is given to

- a) the processes with both District Council partners and contractors for two-way correcting of inaccurate data; and
- b) the lawful bases for all data processing activities are established and documented where appropriate.

Priority Score

2

Agreed Action

Timescale

December 2021

SWP have met with SCC's Data Protection Officer (DPO) to understand the scale of work involved in undertaking a Record of Processing Activity (ROPA). It is clear that this is an in-depth piece of work which will need to be led by SCC's DPO. This is now reflected in the workplan for SCC's Data Protection Officer, but given other pressures and the time this takes it is likely to take approximately 12 months to complete. It is understood that SCC have not completed a ROPA themselves yet, so SWP's completion of this should support wider partnership efforts to review the completeness of their GDPR compliance. SWP's Strategic Management Group (SMG) with partner officers will act as project board, with SCC's DPO liaising with her peers in District Councils as appropriate throughout the process.

Responsible Officer

SCC Data Protection Officer/ SWP Managing Director/SCC legal (Project managed by SWP Business Support Manager)

1.3 Finding and Action

Issue

Risk

No information audit has been conducted and there has been only limited consideration of all personal data collected, held, and transmitted by the Waste Partnership.

Non-compliance with the GDPR may in the first instance result in a warning from the Information Commissioner's Office and could also result in reputational damage.

Findings

Aside from the data held by the Waste Partnership from the Council Tax records of each of the District Councils in Somerset, there are other personal data sets that are held and transmitted to third parties for a number of other bespoke services. These services have various ways that customer requests can be made,

either online or by phone, to either the Waste Partnership or the District Councils.

We considered all bespoke services and the extent to which customers are informed about how the personal data they submit is managed. The findings are:

Service	What customers are informed when they request the service
Garden Waste	The Terms & Conditions webpage does not inform customers that their data is shared with neither the contractor who issues the container stickers, or with the contractor for the collection service.
Household Waste Centre Permits for trade vans and trailers to dispose of concrete and plasterboard	The Terms & Conditions webpage does not inform customers that their data is shared with the contractor who issues the permits.
Clinical waste collection	There has been no assessment of the actual data collected when a service request is made, or what is shared with contractors, in terms of whether the customer is notified before the request is processed.
Bulky waste collections	Customers are not told that their data is shared with a contractor if they request either service from SWP and it has not been confirmed what the District Council customer service teams advise customers.
Asbestos collections	There has been no assessment of the actual data that is collected, particularly where it expands on what is already held in the customer database and also what is ordinarily shared with contractors, in terms of whether the customer is notified before the request is processed. Customers are not told that their data is shared with a contractor.
Customer newsletter – the ‘Sorted’ ezine	Customers receive a confirmation email which states: <i>We will keep your e-mail address securely to send you our Sorted ezine and other updates about waste services (including collection day changes after bank holidays). We will not share your data with third parties. Our full Privacy Policy can be found here. You can unsubscribe at any time.</i> This information is inaccurate because customer data is shared with a third party*

*For the SWP ‘Sorted’ ezine, customer’s personal data is currently transmitted to another EU member state, in that the organisation that produces its newsletters are based in Italy. The Waste Partnership are in the process of procuring a new, domestic, supplier for this service. Whilst the existing arrangement remains in place, customers signing up to receive the newsletter need to be given more specific information about how their privacy is protected.

For customers requiring an assisted collection, their names and addresses are currently shared with the collections contractor and it has been questioned whether this data may require a higher level of protection if it relates to the disability status of a customer. The contractor themselves previously raised this as a GDPR

concern. SWP referred it to the SCC Information Governance Manager who they believe confirmed that the process is GDPR compliant, but they have no confirmation of the clearance.

A Record of Processing Activity (ROPA) format has been recommended by the SCC Data Protection Officer as a means of collating information about and assessing all data processing activity for compliance with GDPR requirements. The outcomes of this exercise may also identify the need for specific Data Protection Impact Assessments (DPIAs) to be conducted, which the GDPR requires for any system or project which presents a 'high risk to individuals' rights and freedoms'.

The Waste Partnership's current website also has a privacy notice states that *"Information required to provide services will also be passed to the organisation contracted to deliver that service."*

This is not sufficiently detailed and needs to be expanded to explain precisely what information is shared, what services this statement includes, and which contractors are being referred to. Furthermore, the privacy notice only covers information that is transacted via the SWP website and all other data transactions need to be covered by separate and specific privacy notices.

It is acknowledged that with the implementation of My Waste Services, customer requests via the website will be expanded and adjusted and this provides an opportunity to ensure GDPR compliance with information provided to customers.

Recommendation

We recommend that the SCC Data Protection Officer should work with the Waste Partnership to ensure that as part of completing a Record of Processing Activity, all bespoke services provided by the Waste Partnership are subject to full and formal assessment. This will identify where data transfers require specific Data Protection Impact Assessments to be conducted.
Remedial actions should be taken in respect of the data sharing activities identified to ensure that customers are fully informed with regards to how their data is used, stored and transmitted.

Priority Score

2

Agreed Action

As above – this will form part of completing the Record of Processing Activity.
Garden Waste subscription service terms and conditions will be thoroughly reviewed with SCC's Data Protection Officer and legal ahead of the commencement of the next (2021) subscription year.

Timescale
Responsible Officer

December 2021
SCC Data Protection Officer/ SWP Managing Director (Project managed by SWP Business Support Manager)

Recommendation

We recommend that the SCC Data Protection Officer should work with the Waste Partnership to ensure that a review is conducted of the privacy notice on the SWP website for compliance with the GDPR

Priority Score

2

requirements, which can be found at: https://ico.org.uk/for-organisations/data-protection-self-assessment/what-information-you-must-supply-under-the-gdpr/		
Agreed Action	Timescale	January 2021
Privacy notices are in place need review. SCC's Data Protection Officer has already commenced this review with partner DPOs at District Councils. SCC's Data Protection Officer will review all existing privacy notices and develop/strengthen or add to them, drawing on the good practice that already exists (for examples Mendip District Council's format has been initially identified as a good format to utilise more consistently across all partners). As each partner may have their own style and format whilst there may be presentational differences, the aim will be to ensure that there is full consistency with all notices in terms of content and compliance. SCC's Data Protection Officer will review draft revised privacy notices with SWP before securing sign-off from all partner DPOs and SMG to the revised notices.	Responsible Officer	SCC's Data Protection Officer/SWP Managing Director

1.4 Finding and Action	
Issue	Risk
There has been no formal consideration of services where data subject consent is required for their personal information to be held, how it is obtained and how business processes are designed to ensure that the rights of the individual can be delivered.	Non-compliance with the GDPR may in the first instance result in a warning from the Information Commissioner's Office and could also result in reputational damage.
Findings	
<p>The GDPR requires that, when obtaining consent from data subjects for their data to be held and used, organisations must ensure the process is specific, granular, clear, prominent, opt-in only, documented and easily withdrawn. The key points are:</p> <ul style="list-style-type: none"> * Unbundled: consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service. * Active opt-in: pre-ticked opt-in boxes are invalid – use unticked opt-in boxes or similar active opt-in methods (e.g. a binary choice given equal prominence). * Granular: give granular options to consent separately to different types of processing wherever appropriate. * Named: name the authority and any third parties who will be relying on consent – even precisely defined categories of third-party organisations are not acceptable under the GDPR. <p>SWP must review how they seek, record and manage consent, so that customers have a genuine choice and control over how they use their data. The review</p>	

needs to particularly consider whether they have implemented appropriate mechanisms in order to ensure an effective audit trail of consent.

SWP should also review their procedures to ensure that they can deliver an individuals' rights as required under the GDPR, which include:

- * The right to be informed;
- * the right of access;
- * the right to rectification;
- * the right to erasure;
- * the right to restrict processing;
- * the right to data portability;
- * the right to object; and
- * rights in relation to automated decision making and profiling.

In particular, there are important considerations to make regarding the right to rectification. In terms of who has responsibility for inaccurate name and address data provided by District Councils, SWP need to consider whether there is a mechanism to ensure that regardless of which organisation the customer notifies, that both the Council Tax and Waste databases are corrected, as recommended under paragraph 1.9.

In order to deliver the remaining rights, SWP need to establish how their back-end systems arrangements support compliance with the GDPR and this should appear in the Privacy Notices.

Recommendation

<p>We recommend that the SCC Data Protection Officer should work with the Waste Partnership to ensure that as part of completing the Record of Processing Activity, consideration is given to</p> <ol style="list-style-type: none"> a) appropriate arrangements for when SWP should seek, record and manage consent from data subjects for their data to be processed; b) how processes have been designed to ensure they can deliver the rights of the individual as required by the GDPR. 	<p>Priority Score</p>	<p>2</p>
<p>Agreed Action</p>	<p>Timescale</p>	<p>December 2021</p>
<p>As above – this will form part of completing the Record of Processing Activity.</p>	<p>Responsible Officer</p>	<p>SCC Data Protection Officer/ SWP Managing Director (Project managed by SWP Business Support Manager)</p>

1.5 Finding and Action

Issue	Risk
<p>It is unknown to what extent all relevant policy guidance has been communicated to SWP staff and there are no arrangements for the monitoring of policy compliance.</p> <p>GDPR refresher training has not been made available to SWP staff and may not include all relevant areas.</p>	<p>Without periodic training, staff may have insufficient knowledge regarding GDPR requirements and their own responsibilities for ensuring compliance.</p>
<p>Findings</p>	
<p>A key part of an organisation's GDPR compliance framework is its data protection policies. This should translate the legislative requirements of the GDPR to staff required to adhere to it in a clear manner. To ensure staff are aware of, and remain compliant with policy framework, the appointed Data Protection Officer should conduct regular audits of compliance and address any issues identified.</p> <p>However, because of the previous lack of clarity regarding the arrangements for a Data Protection Officer for the Waste Partnership, there has not been any formal arrangements for the monitoring of policy compliance. This should include regular reviews of the effectiveness of data handling and processing activities and security controls.</p> <p>It is recommended by the ICO that Authorities implement appropriate technical and organisational measures that ensure and demonstrate that they comply. These measures can include internal data protection policies, staff training, internal audits of processing activities and reviews of internal HR policies. Practically, this has meant for some that more policies and procedures must be developed. However, if SCC already has good governance measures in place, then it should not be onerous to ensure that the same measures can be implemented for the Waste Partnership.</p> <p>We have obtained assurances that as the administering authority, Somerset County Council has set out the management support and direction for data protection compliance in a framework of policies and procedures. This includes a suite of documents covering data protection, information security and data breaches.</p> <p>With SCC as the administering authority for SWP, they would be expected to adopt and comply with the SCC procedures to ensure personal data breaches are detected, reported and investigated effectively. SCC have a Data Breach Policy dated 2018. However, there is a lack of clarity as to whether it has been communicated to SWP staff because the procedures are not included within current available training.</p> <p>The policy should be reviewed for adequate mechanisms in place to both assess and then report relevant breaches to the ICO where the individual is likely to suffer some form of damage e.g. through identity theft or confidentiality breach. This should also include what mechanisms need to be in place to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms. The policy should then be rolled out to all staff.</p> <p>Staff also need to complete training on how to identify both a Freedom of Information and Data Subject Access requests and the Business Support Manager advised that as this is not currently included within SCC GDPR training, there is a likelihood that many staff will not have received any training in this area since their induction period.</p> <p>It is also understood that annual refresher training is the normal requirement. However, it has not yet been launched by The Learning Centre and as such, there</p>	

<p>has been no reminder issued for staff to complete a refresher, despite the SWP Business Support Manager having chased for an update. The available training does not yet provide staff with any understanding of the GDPR implications of SharePoint, which is being implemented.</p>		
<p>Recommendation</p>		
<p>We recommend that the SCC Data Protection Officer should liaise with the Waste Partnership to ensure that consideration is given to how SCC corporate arrangements for the monitoring and assurance of compliance with the GDPR Policy framework can also provide assurance for SWP.</p>	<p>Priority Score</p>	<p>2</p>
<p>Agreed Action</p>	<p>Timescale</p>	
<p>Helen to discuss with Lucy</p>	<p>Responsible Officer</p>	
<p>Recommendation</p>		
<p>We recommend that the SCC Data Protection Officer ensures that refresher training for GDPR via The Learning Centre is provided. This should also include consideration of whether there is sufficient coverage and understanding of the GDPR implications of SharePoint, the Data Breach Policy and also the processes for identifying and responding to Freedom of Information and Data Subject Access Requests.</p>	<p>Priority Score</p>	<p>2</p>
<p>Agreed Action</p>	<p>Timescale</p>	<p>By December 2021 (inc 2020/21 annual appraisal cycle in Spring/Summer 2021), and immediately for new joiners</p>
<p>SWP staff have completed all training and followed all processes as required to be our administering authority (SWP). SCC have developed a new training module which addresses the gaps identified above and this is now available to SWP staff. Compliance with this will be checked by SCC through the annual staff appraisal process and has been embedded in SCC's induction process for new staff.</p> <p>SWP have requested that SCC's Data Protection Officer put in place meta compliance on all Data Protection and GDPR policies (monthly if there are updates). This will ensure full compliance as staff will be required to certify that they have read the update before they are able to logon.</p>	<p>Responsible Officer</p>	<p>SCC's Data Protection Officer/SWP's Business Support Manager</p>

1.6 Finding and Action		
Issue	Risk	
Arrangements for how a Data Subject Access Request would be managed are yet to be defined and staff have not received training on how to identify and channel a request.	Non-compliance with the GDPR may in the first instance result in a warning from the Information Commissioner's Office and could also result in reputational damage.	
Findings		
<p>SWP have never received a data subject access request but are still required by the GDPR to have plans in place for how they will handle requests from individuals for access to their personal data within the new timescales outlined in the GDPR. This will need to include how they will provide any additional information to requestors as required under the GDPR.</p> <p>The new rules are:</p> <ul style="list-style-type: none"> * In most cases they will not be able to charge for complying with a request. * They have a month to comply. * They can refuse or charge for requests that are manifestly unfounded. Excessive requests can also be charged for or refused. * Where they refuse to respond to a request, they must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month. <p>SCC have defined procedures and a system in which requests are recorded and monitored. The Waste Partnership do not currently have access to system and whether the procedures are suitable for them to adopt has not been assessed. A recommendation has been raised above for staff to receive training on how to identify and channel a request, should they receive one.</p>		
Recommendation		
We recommend that the SCC Data Protection Officer should liaise with the SWP Managing Director should ensure there are sufficient arrangements in place for how the Waste Partnership will handle requests from individuals for access to their personal data within the timescales outlined in the GDPR, including how they will provide any additional information to requestors as required under the GDPR. This can be achieved by exploring whether SCC processes are sufficient and can be adopted.	Priority Score	3
Agreed Action	Timescale	By December 2021 (inc 2020/21 annual appraisal cycle in Spring/Summer 2021), and immediately for new joiners

<p>SCC have now updated their GDPR training to include training on these processes. This will be rolled out to staff through the training and meta-compliance processes set out above.</p> <p>SCC's Data Protection Officer has now made access to the system which manages such requests.</p>	<p>Responsible Officer</p>	<p>SCC's Data Protection Officer/SWP's Business Support Manager</p>
--	----------------------------	---

Findings and Actions for Somerset Waste Partnership

1.7	Finding and Action	
Issue	Risk	
The allocation of key responsibilities to ensure GDPR compliance has not been completed in a timely manner.	SWP will continue to be non GDPR compliant and moving forwards GDPR will not be considered as part of future business improvement projects.	
Findings		
<p>In addition to the Data Protection Officer not being routinely involved with SWP, we have also identified that the SCC IT Enterprise Architect who works with SWP does not periodically attend any SWP business meetings. He is instead called up as and when necessary to consult on specific ICT projects, as identified by SWP managers. This approach may result in insufficient involvement and oversight if SWP staff do not fully understand the technical implications of all business decisions, to determine when involvement is required. An example was identified whereby the IT Enterprise Architect was unaware whether the My Waste Services system implementation had been subject to a Data Protection Impact Assessment, which arguably should have required his input. Further considerations required are also reported under paragraph 1.8.</p> <p>SWP are however due to implement a new project management approach that will better define the appropriate involvement of experts in projects.</p> <p>The SWP Business Support Manager assumed responsibility for oversight of GDPR compliance arrangement in early 2019 and has to date, received no enhanced training despite this role only being agreed post the GDPR implementation date. Given that the availability of the SCC IT Enterprise Architect and DPO are limited and practically they would be unable to attend all Senior Leadership meetings, the ability of the SWP Business Support Manager to identify all operational developments that have relevant GDPR considerations is crucial. This will ensure that other individuals can be engaged at the right time and with the appropriate level of involvement.</p>		
Recommendation		

<p>We recommend that the Waste Partnership Managing Director should ensure that</p> <p>a) the new approach to project management at SWP will define and ensure that the IT Enterprise Architect is appropriately involved in SWP operational decisions, so that they have an awareness of business processes and are able to advise on data protection from a technical perspective; and</p> <p>b) the Business Support Manager attends suitable training that is appropriate for her data controller role. The training should ensure she is familiar with all GDPR implications and how they relate to SWP operations, including the lawful basis for processing personal data, including consent, maintaining the rights of individuals and the process for breach notifications.</p>	<p>Priority Score</p>	<p>2</p>
<p>Agreed Action</p>	<p>Timescale</p>	<p>December 2021</p>
<p>SWP will update SWP's project management processes (the Project Initiation Document template) to ensure that the potential need for the input of SCC's DPO or IT Enterprise Architect is identified at the outset of considering a new project. For example, in the project to centralise garden waste payments, regular calls with SCC's ICT Enterprise Architect have been arranged.</p> <p>Having reviewed available training options for SWP's Business Support Manager SWP have been unable to identify a suitable training course – one that is more than a general awareness but less than the training a DPO would require. SWP have agreed the SCC's DPO will provide SWP's Business Support Manager with training (through a number of sessions as it is an extensive area), with a follow up session to involve other members of SWP's Business Support and Customer Service team so that we have back-up and strength in depth.</p>	<p>Responsible Officer</p>	<p>SCC's Data Protection Officer/SWP's Business Support Manager</p>

<p>1.8 Finding and Action</p>	
<p>Issue</p>	<p>Risk</p>
<p>It is unclear how it will be ensured that SWP's use of technology for all services provided is, and will continue to be, GDPR compliant.</p>	<p>Non-compliance with the GDPR may in the first instance result in a warning from the Information Commissioner's Office and could also result in reputational damage.</p>
<p>Findings</p>	
<p>We have been unable to fully verify whether all technology requirements and considerations have been identified and assessed for compliance with the articles of the GDPR, with sufficient engagement from the IT Enterprise Architect as reported above.</p>	

We have been able to obtain some specific assurances for My Waste Services, including the back-end operation of the system and the provider’s commitment to GDPR compliance, because this is a current project. However, when we enquired about other elements of the project, such as the data interface between MWS and the system of the new contractor Suez, there was less certainty.

The Waste Partnership website, SharePoint and Outlook are all maintained by SCC, which gives increased assurance, but there has been a lack of transparency of the extent to which technical configurations provide GDPR compliance, or if any further actions are required.

For other elements of the business and data management there will need to be specific consideration given to the technology requirements for all services provided (as listed under paragraph 1.3 in this report).

For specific services and processes, this should include: -

1. Processes regarding Data Acquisition and Processing – including explicit consent to acquire and process personal data
2. Processes regarding Data Storage – including protection of data from destruction, loss, alteration, unauthorised disclosure, dissemination, or access
3. Processes regarding Data Movement – including secure data during transmissions and transfer of personal data between service providers
4. Processes regarding Data Retention and Disposal – including data availability and recovery from disaster
5. Processes regarding Monitoring, Verification and Alerts – including assessment and notification within 72 hours of personal data breach.

Recommendation

We recommend the SWP Managing Director should engage the SCC IT Service to conduct a review of SWP’s use of IT, to ensure it is compliant with the requirements of the GDPR.

Priority Score

2

Agreed Action

Timescale

December 2021

SCC ICT have been involved in all major projects when SWP has procured and installed new ICT systems. The ROPA which SWP/SCC’s Data Protection Officer will include a review of SWP’s use of ICT. However, where SWP simply uses systems maintained by the County Council (for example Sharepoint and Outlook) then SWP will not undertake a separate review of these systems, and instead SCC’s Data Protection Officer will, in conjunction with SCC ICT, agree the most effective way of reviewing use of these systems across SCC.

Responsible Officer

SCC Data Protection Officer/ SWP Managing Director (Project managed by SWP Business Support Manager)

1.9 Finding and Action		
Issue	Risk	
<p>The information sharing agreement between the Waste Partnership and its District Council partners does not meet GDPR requirements.</p> <p>Data subjects are not notified that their personal information is shared with the Waste Partnership, or its contractors when they register for Council Tax purposes with District Councils.</p>	<p>Non-compliance with the GDPR may in the first instance result in a warning from the Information Commissioner's Office and could also result in reputational damage.</p>	
Findings		
<p>The origin of the largest part of the data held by the Waste Partnership, is from the Council Tax records of each of the District Councils in Somerset. When a citizen registers for Council Tax or updates their address, the data they provide is automatically passed to the Waste Partnership for waste and recycling collections to commence.</p> <p>SWP have recently agreed with the County and District Councils that they will be joint data controllers of this information and this will be formalised by a new inter-authority agreement, due to be approved by the Waste Board.</p> <p>Advice provided by the SCC Legal Team was reviewed and has made suitable recommendations for the revisions needed to the over-arching Inter Authority Agreement. However, the changes are yet to be actioned.</p> <p>The District Councils have a responsibility to notify their citizens that when they provide their personal information for Council Tax purposes, that it is then shared with SWP and their contractors for waste collection and recycling purposes. This can be partially achieved via the privacy notices on the website of the District Councils, for those citizens who submit their information online.</p> <p>The current privacy notices were reviewed by SWP during the course of the audit and found to be variable and generally lacking in clarity regarding this specific data transfer. The structure of the SWP Management Group provides an opportunity for this issue to be raised with and addressed by District Council representatives and an SCC template Privacy Notice has been provided to SWP as part of the audit.</p>		
Recommendation		
<p>We recommend that the Waste Partnership Managing Director should ensure that the Inter Authority Agreement is revised in line with the advice provided by the SCC Legal Team.</p>	Priority Score	2
Agreed Action	Timescale	December 2021
<p>Legal advice that SWP obtained from SCC legal has set out that that SWP and each District Council will be joint controllers of the data that is collected by the DCs for SWP. This is because the parties have decided together the reasons for collecting the data and how it will be collected and used. The DCs cannot be sole controllers of the data because they have assigned their waste collection duties to SWP – they are</p>	Responsible Officer	SWP Managing Director

controllers only by virtue of the fact that they will collect and process the data in order to deliver statutory services that they have not delegated. Joint controllers have to set out their respective roles and responsibilities in an agreement and the GDPR says that joint controllers are jointly liable for compliance with the rules on data processing.

A variation to the Inter Authority Agreement will be required to document the respective role and responsibilities of partners and SWP, as data handling by the DCs has consequences for SCC's performance of its obligations under the IAA. This will be developed by legal, with suitable input from SWP and SCC's Data Protection Officer. SWP's constitution allows for changes of this nature to the IAA to be undertaken with the written agreement of each partner authority Chief Executive, rather than automatically requiring this to be taken through each partners full council or cabinet. SMG have previously indicated their preference for this change to be undertaken through this method and this approach has been reviewed by community governance. Should any partner have any concerns when written agreement is sought then the constitution has suitable processes in place to ensure any such concerns are adequately dealt with.

The timescale for this activity is set so that we can ensure that any amendments required as a result of completing the ROPA can be reflected in the variation to the Inter Authority Agreement.

Recommendation

We recommend that the Waste Partnership Managing Director should ensure that District Council partners are informed of the need to update their website privacy notices and make other relevant arrangements, so that citizens are informed that registering for Council Tax means their data is shared with the Waste Partnership and their contractors for waste and recycling collection purposes.

Priority Score

2

Agreed Action

Timescale

December 2021

Privacy notices are in place need review. SCC's Data Protection Officer has already commenced this review with partner DPOs at District Councils. SCC's Data Protection Officer will review all existing privacy notices and develop/strengthen or add to them, drawing on the good practice that already exists (for examples Mendip District Council's format has been initially identified as a good format to utilise more consistently across all partners). As each partner may have their own style and format whilst there may be presentational differences, the aim will be to ensure that there is full consistency with all notices in terms of content and compliance. SCC's Data Protection Officer will review draft revised privacy notices with SWP before securing sign-off from all partner DPOs and SMG to the revised notices.

Responsible Officer

SCC's Data Protection Officer/SWP Customer Experience Manager



1.10 Finding and Action		
Issue	Risk	
Some actions to raise awareness and engagement with staff regarding GDPR changes to personal data management have not been fully implemented.	Non-compliance with the GDPR may in the first instance result in a warning from the Information Commissioner's Office and could also result in reputational damage.	
Findings		
<p>In the pre-implementation stages prior to GDPR becoming law, the SWP Business and Governance Manager, who was responsible for GDPR readiness had issued email communications to staff requesting that they checked their own personal folders on the network drive and also notified management of all customer databases held outside of the main system. This was to include customer personal data in personal folders and details of all customer databases held.</p> <p>However, the SWP Business and Governance Manager left his post in August 2018 and there is no evidence that the outcomes of these requests were followed up, with necessary actions completed.</p> <p>The forthcoming implementation of SharePoint will address data within personal folders as it will include a data cleanse exercise in line with a revised data retention policy. However, this will not address personal data held within Outlook, which will require personal management by staff.</p>		
Recommendation		
We recommend that the Waste Partnership Managing Director ensures that staff are given appropriate guidance on how to manage personal data contained within emails, so that retention periods are enforced to ensure GDPR compliance.	Priority Score	3
Agreed Action	Timescale	Summer 2021
As set out above, SWP will ensure that our staff undergo the revised GDPR training module developed by SCC this year. A policy on managing personal data contained within emails for SWP will be developed by SCC's Data Protection Officer.	Responsible Officer	SCC's Data Protection Officer/SWP's Business Support Manager

1.11 Finding and Action		
Issue	Risk	
Contractual agreements between the Waste Partnership and its service providers do not adequately reference GDPR responsibilities or arrangements.	Non-compliance with the GDPR may in the first instance result in a warning from the Information Commissioner's Office and could also result in reputational damage.	
Findings		
Customer data to facilitate the provision of all waste and recycling services is shared with SWP's current contractors - Viridor for waste disposal and Kier for collections.		
The contracts for Kier was obtained and reviewed, which identified that it has not been updated in line with GDPR and makes no reference to it - it only includes data protection clauses. The contract should have been updated to reference the GDPR rather than the Data Protection Act and should also set-out the GDPR compliance arrangements the organisation has in place, such as the Data Protection Officer.		
Amending the Kier contract is not considered necessary due to its imminent expiry. The collections contract will be assumed by Suez in April 2020 and a review of the data protection clauses as part of this audit confirmed it to be sufficient.		
The Viridor contract was also reviewed and found to include a variation, which changes all reference to the Data Protection Act to the GDPR. It does not however set-out the GDPR compliance arrangements the organisation has in place, such as the Data Protection Officer.		
However, SWP should first establish the current position of the Information Commissioners Office, on allowing data processors to wait until contracts are due for renewal before making such changes. This is a changeable position and is being frequently updated based on emerging case law.		
Recommendation		
We recommend that the Waste Partnership Managing Director should ensure that the Viridor contract variation for GDPR should be expanded to specify all data protection compliance arrangements.	Priority Score	3
Agreed Action	Timescale	Spring 2021
SWP will follow the advice of SCC's Data Protection Officer in whether to amend the Viridor contract or wait until the contract is due for renewal. Appropriate legal advice was taken when formulating the collection contract with Suez.	Responsible Officer	SCC's Data Protection Officer/SWP's Treatment & Infrastructure Contract

		Manager
--	--	---------

1.12 Finding and Action		
Issue	Risk	
Initial GDPR staff training has not been completed by all SWP employees.	Staff may have insufficient knowledge regarding GDPR requirements and their own responsibilities for ensuring compliance.	
Findings		
We have been provided with evidence that the majority of Waste Partnership staff have completed specific online GDPR training via SCC's Learning Centre, between May and July 2018. At the time of reporting, there were however two newer staff members who have not yet completed training.		
Recommendation		
We recommend that the Waste Partnership Managing Director should review the new members of staff who are still to complete initial training.	Priority Score	3
Agreed Action	Timescale	Spring 2021
Only 2 out of 24 staff had not completed the training. All staff to do new SCC GDPR training (as set out above) and SWP to include this in our induction process for new staff	Responsible Officer	SWP's Business Support Manager

Other Suggestions

We recommend that SWP should add an entry to the SWP risk register for the risk of data loss and ensure that it is subject to regular monitoring. This should include the identification and inclusion of any areas that could cause compliance problems under the GDPR.

Audit Framework and Definitions



SWAP work is completed to comply with the International Professional Practices Framework of the Institute of Internal Auditors, further guided by interpretation provided by the Public Sector Internal Auditing Standards.

Assurance Definitions

None	The areas reviewed were found to be inadequately controlled. Risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
Partial	In relation to the areas reviewed and the controls found to be in place, some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
Reasonable	Most of the areas reviewed were found to be adequately controlled. Generally, risks are well managed but some systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
Substantial	The areas reviewed were found to be adequately controlled. Internal controls are in place and operating effectively and risks against the achievement of objectives are well managed.

Definition of Corporate Risks

Risk	Reporting Implications
High	Issues that we consider need to be brought to the attention of both senior management and the Audit Committee.
Medium	Issues which should be addressed by management in their areas of responsibility.
Low	Issues of a minor nature or best practice where some improvement can be made.

Categorisation of Recommendations

In addition to the corporate risk assessment it is important that management know how important the recommendation is to their service. Each recommendation has been given a priority rating at service level with the following definitions:

Priority 1	Findings that are fundamental to the integrity of the service’s business processes and require the immediate attention of management.
Priority 2	Important findings that need to be resolved by management.
Priority 3	Finding that requires attention.

Authors and Distribution



Please note that this report has been prepared and distributed in accordance with the agreed Audit Charter and procedures. The report has been prepared for the sole use of the Partnership. No responsibility is assumed by us to any other person or organisation.

Report Authors

This report was produced and issued by:

Lisa Fryer	Assistant Director
Jenny Frowde	Principal Auditor

Distribution List

This report has been distributed to the following individuals:

Mickey Green	Managing Director
Helen Oaten	Business Support Manager
Rebecca Martin	Service Manager - Customer Experience & Information Governance